UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

TRAVIS JAMES, STEFANIE SHEEHAN, KIMBERLY GAMBOA, and KOREY WILLIAMS, individually and on behalf of all others similarly situated, Plaintiffs, v. DAVACO, INC. and DAVACO LP, Defendants.	Case No. 3:21-cv-02318-M **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL COMPLEX

Plaintiffs Travis James, Stefanie Sheehan, Kimberly Gamboa, and Korey Williams ("Plaintiffs") bring this Consolidated Class Action Complaint against Davaco, Inc. and Davaco LP ("Defendants") in their individual capacities and on behalf of all others similarly situated (the "Class," defined *infra*), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Personally Identifiable Information ("PII") Defendants required from their employees as a condition of employment, including without limitation, names, Social Security numbers, and driver's license numbers or government-issued identification numbers

(collectively, "Sensitive Information"). Defendants confirmed the Sensitive Information was accessed and taken by an unknown and unauthorized individual.[1]

2. Defendants comprise a multi-site project management and deployment company supporting retail, restaurant, and hospitality services with the development, transformation, and maintenance of clients' physical sites.

3. Part of Defendants' business involves collecting and storing confidential employee information.

4. Plaintiffs and all other persons similarly situated had a right to keep the Sensitive Information they provided to Defendants confidential. Plaintiffs and other members of the Class (as defined *infra*) relied on Defendants to keep their Sensitive Information confidential as required by the applicable laws.

5. Defendants violated this right. They failed to implement or follow reasonable data security procedures as required by law, and failed to protect Plaintiffs and Class members' Sensitive Information from unauthorized access.

6. As a result of Defendants' inadequate data security and inadequate or negligent training of their employees, on or around June 11, 2021, Defendants were alerted to suspicious activity on their computer network. On or before June 11, 2021, Plaintiffs' and Class members' Sensitive Information—including their name, Social Security number, and Driver's license or government issued identification—was accessed, viewed, and taken by unauthorized and unknown person(s) as part of a ransomware attack and exfiltration of data ("Data Breach"). On or about June 15, 2021, Defendants confirmed this unauthorized access.

[1] *See Notice of Data Security Incident*, available at: https://www.doj.nh.gov/consumer/security-breaches/documents/davaco-20210716.pdf ("Davaco confirmed that the data viewed or taken by the attacker included employees' personal information.") (last accessed Dec. 20, 2021).

7. On information and belief, on or around July 2, 2021, Defendants provided notice of the Data Breach to approximately 14,578 current and former employees—including Plaintiffs.[2] The notice stated that on June 11, 2021, Defendants' were alerted to suspicious activity on their network that ended up being an authorized individual (or "attacker") accessing their network, and the attacker instigated a ransomware attack, and viewed and removed data stored in Defendants' system containing employee sensitive and confidential Sensitive Information—including their name, Social Security number, and Driver's license or government issued identification.

8. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect their employees' Sensitive Information.

9. Defendants disregarded the rights of Plaintiffs and Class members by, among other things:

a. recklessly or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions;

b. failing to disclose that they did not have reasonable or adequately robust computer systems and security practices to safeguard their employees' Sensitive Information;

c. failing to take standard and reasonably available steps to prevent the Data Breach;

d. failing to monitor and timely detect the Data Breach; and

[2] *See* State of Maine Data Breach Notification Information, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/07bf9dbb-2a4a-47d4-9530-1a0d446b5c6c.shtml (last visited Jan. 3, 2022).

e. failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

10. As a result of Defendants' failure to implement and follow reasonable security procedures, Plaintiffs' and Class members' Sensitive Information is now in the hands of thieves. Plaintiffs and Class members have spent, and will continue to spend, significant amounts of time and money trying to protect themselves from the adverse ramifications of the Data Breach and dealing with actual fraud and will forever be at a heightened risk of identity theft and fraud.

11. Plaintiffs, on behalf of all others similarly situated, allege claims for (1) negligence; (2) invasion of privacy; (3) breach of implied contract; (4) unjust enrichment; (5) breach of fiduciary duty; (6) breach of confidence; (7) declaratory and injunctive relief; (8) violation of the California Consumer Privacy Act (Cal. Civ. Code § 1798.150); (9) violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq*.). Plaintiffs and the Class members seek damages, including but not limited to nominal and treble damages from Defendants, and to compel Defendants to adopt reasonably sufficient security practices to safeguard Plaintiffs' and Class members' Sensitive Information that remains in Defendants' custody to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

A. Plaintiffs.

12. Plaintiff Travis James is a resident of the Commonwealth of Pennsylvania and was employed by Defendants. Plaintiff James received notice from Defendants that his Sensitive Information had been improperly exposed to unauthorized third parties, and is acting on his own behalf and on behalf of others similarly situated.

13. Plaintiff Stefanie Sheehan is a resident of the State of California and was employed by Defendants. Plaintiff Sheehan received notice from Defendants that her Sensitive Information had been improperly exposed to unauthorized third parties, and is acting on her own behalf and on behalf of others similarly situated.

14. Plaintiff Kimberly Gamboa is a resident of the State of California and was employed by Defendants. Plaintiff Gamboa received notice from Defendants that her Sensitive Information had been improperly exposed to unauthorized third parties, and is acting on her own behalf and on behalf of others similarly situated.

15. Plaintiff Korey Williams is a resident of the State of Louisiana and was employed by Defendants. Plaintiff Korey Williams received notice from Defendants that his Sensitive Information had been improperly exposed to unauthorized third parties, and is acting on his own behalf and on behalf of others similarly situated.

B. Defendants.

16. Defendant Davaco, Inc. was founded in 1990, and is a corporation organized under the laws of the State of Texas, with U.S. operations headquartered in the Dallas–Fort Worth Metroplex, at 4050 Valley View Lane, Suite 150; Irving, Texas 75038.

17. Defendant Davaco LP is a limited partnership organized under the laws of Delaware and with its headquarters located at 6688 North Central Expwy, Suite 1400, Dallas, Texas 75206.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to

reflect the true names and capacities of such other responsible parties when their identities become known.

19. Plaintiffs' claims stated in this complaint are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class, defined *infra*, is a citizen of a different state than Defendants, and there are more than 100 putative Class members.

21. The Northern District of Texas has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in Texas and this District through their headquarters, offices, parents, and affiliates.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or their parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs claims occurred in this District.

FACTUAL ALLEGATIONS

C. Background.

23. Defendants are a leading provider of customized logistics solutions. Davaco specifically provides support to clients with multi-site project management and resource deployment for the development, transformation, and maintenance of physical sites, and employs over 1,700 employees across North America.[3] Davaco also develops business solutions such as

[3] *See* https://www.davaco.com/about (last accessed Dec. 28, 2021).

graphic installations, project management, hard line and soft line merchandising, marketing surveys, and logistics for retail, restaurant, and hospitality businesses throughout the United States.

24. Defendants required their employees—including Plaintiffs and Class members—to provide Defendants with Sensitive Information, including their names, dates of birth, Social Security numbers, driver's license or other government issued identification numbers, and other sensitive and confidential information, which is static, does not change, and in the hands of criminals can be used to commit myriad financial and other crimes.

25. Plaintiffs and Class members, as current and former employees, relied on these sophisticated Defendants to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class members demand security to safeguard their Sensitive Information.

26. Defendants had a duty to adopt reasonable, appropriate, industry standard, and/or legally required measures to protect Plaintiffs' and Class members' Sensitive Information from unauthorized disclosure or dissemination to unauthorized third parties without their express, written consent, as further detailed below.

D. The Data Breach.

27. On June 11, 2021, Defendants became aware of suspicious activity on their computer network.[4] Defendants then engaged cybersecurity experts and computer forensic

[4] State of California Department of Justice, *Submitted Breach Notification Sample*, available at: https://oag.ca.gov/ecrime/databreach/reports/sb24-543040 (last accessed Jan. 7, 2022).

investigators to help investigate the suspicious activity. Defendants confirmed an unauthorized individual gained access to their computer network and conducted a ransomware attack.[5]

28. On or about June 15, 2021, Defendants confirmed the unauthorized individual (s) also viewed and took data from their system—and that data included Plaintiffs' and Class members' Sensitive Information.[6]

29. On or around July 2, 2021, Defendants issued a Notice of Data Event, notifying employees of an incident involving potential unauthorized access to unencrypted personal information.[7] Defendants provided this Data Breach Notification to approximately 14,578 individuals.[8] The Data Breach notice informed the affected members that their Sensitive Information, specifically their name, Social Security number, and Driver's license or government issued identification number, were part of a ransomware attack, and viewed and taken by an unauthorized party.[9]

30. As of the filing of this complaint, and on information and belief, Defendants have not posted any notice of the Data Breach on their websites.

31. Defendants failed to put in place proper security protocols to protect against the unauthorized release of patient information and failed to properly train their employees on such protocols, resulting in the unauthorized release of private data. As a result of Defendants'

---

[5] *Id.*
[6] *Id.*
[7] It is clear that the information exposed in the Data Breach was unencrypted. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendant notified the California Attorney General of the Data Breach on July 2, 2021, evidencing that the exposed data was unencrypted. *See* State of California *Submitted Breach Notification Sample, supra* note 4.
[8] *See* State of Maine Data Breach Notification Information, *supra* note 2.
[9] State of California Department of Justice, *Submitted Breach Notification Sample, supra* note 4.

failures, Plaintiffs' and Class members' Sensitive Information was subject to a ransomware attack and accessed, viewed, and acquired by unknown and unauthorized third parties and is, or likely will be, for sale on the dark web. This means that the Data Breach was successful in two ways: (1) unauthorized individuals accessed and acquired Plaintiffs' and Class members' unencrypted, unredacted information set forth above; and (2) unauthorized individuals accessed to the computer network and conducted a ransomware attack—a distinct form of data breach, as discussed in further detail *infra*.

32. Plaintiffs and Class members had their Sensitive Information accessed and stolen by an unauthorized party due to Defendants' acts and/or omissions and their failure to properly protect the Sensitive Information they collected, maintained, and used.

33. Defendants should have prevented this Data Breach. Data breaches are a well-known and well publicized problem, thus providing notice to Defendants that the Sensitive Information in their possession could be targeted by unauthorized parties, or "hackers." The Data Breach was the inevitable result of Defendants' inadequate approach and/or attention to data security and protection of the Sensitive Information they collect, maintain, and use in the normal course of business.

34. Defendants disregarded the rights of Plaintiffs and Class members by recklessly, and/or negligently failing to implement industry standard security measures or otherwise take adequate and reasonable measures to ensure protection of their data systems; by failing to disclose the material fact that Defendants did not have adequate computer security systems and practices to safeguard the Sensitive Information they collected, maintained, and used; by failing to take available steps to prevent and stop the breach from ever happening; and by failing to monitor, detect, and stop the breach in a timely manner.

35. As a result of the Data Breach, Plaintiffs' and Class members' Sensitive Information was exposed to and acquired by unauthorized parties—criminals—for misuse, identity theft, and other fraudulent activities. Plaintiffs' exfiltrated Sensitive Information is already being used by unauthorized part(ies) to commit fraud and identity theft, including fraudulent apartment applications (with credit checks), credit card fraud, and fraudulent bank account transactions. The injuries suffered, or likely to be suffered by Plaintiffs and Class members as a direct result of Defendants' Data Breach include, but are not limited to:

a. theft of their personal and financial information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. damages arising from the inability to use their own Sensitive Information;

d. restricted or inability to access their account funds, including the costs and fees associated with inability and/or restrictions on obtaining funds from their accounts or limits on the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. costs, including lost opportunity costs, associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the

stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

f. the current, imminent, and certainly impending injury flowing from ongoing and further potential fraud and identify theft posed by their Sensitive Information being placed in the hands of criminals;

g. the continued risk to Plaintiffs' and Class members' Sensitive Information in Defendants' possession, which remains accessible to Defendants and subject to further breaches so long as Defendants fail to undertake appropriate, reasonable, industry standard, and commercially available measures to protect the Sensitive Information in their possession; and

h. the loss of Plaintiffs' and Class members' privacy.

36. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement and/or maintain adequate data security measures for the Sensitive Information they collect, maintain, and use in the normal course of business.

37. Additionally, Plaintiffs and Class members retain a significant interest in ensuring their Sensitive Information, which—despite being accessed and acquired by an unauthorized party—remains in the possession of Defendants, is protected from further access and acquisition by unauthorized individuals and breaches, and seek to remedy the harms they have suffered, and will continue to suffer, on behalf of themselves and similarly situated individuals whose Sensitive Information was accessed and acquired by an unauthorized party as a result of Defendants' Data Breach.

E. Plaintiffs' Exposure and Mitigation Efforts.

Plaintiff James

38. Plaintiff James was required to provide his Sensitive Information to Defendants in connection with his employment.

39. In or about July 2021, Plaintiff James received notice from Defendants that his Sensitive Information—including his name, Social Security number, and driver's license or government-issued identification number—had been improperly exposed to unauthorized third parties. The notice received by Plaintiff James is substantially similar to the exemplar Data Breach notice letters submitted to the Maine Attorney General, and California and New Hampshire departments of justice.

40. As a direct result of the Data Breach, Plaintiff James has engaged in mitigation efforts and expended time and resources. His efforts include, but are not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by Defendants; researching, signing up for, and paying approximately $20 per month for credit monitoring and identity theft protection services from LifeLock; placing a freeze on his credit with all three bureaus; and contacting creditors and credit bureaus regarding numerous fraudulent attempts by unauthorized third parties to use his name and Social Security number to obtain residential rental contracts. Plaintiff James has spent at least five hours dealing with the Data Breach, valuable time Plaintiff James otherwise would have spent on other activities, including but not limited to work and/or leisure activities.

41. Following the Data Breach, multiple unauthorized third parties attempted to use Plaintiff James's name and Social Security number to secure rental contracts for apartments.

Each attempt, beginning on or about August 26, 2021, and continuing through on or about September 6, 2021, caused various credit bureaus to conduct a "hard pull" on his credit reports. As a result, his credit score was materially and negatively impacted and has yet to recover to its pre-August 26, 2021 level.

42. Knowing that thieves stole his Sensitive Information as part of the Data Breach and knowing that his Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiff James great anxiety. This Data Breach has given Plaintiff James hesitation about using electronic services and reservations about conducting other online activities requiring his personal information.

43. Plaintiff James suffered actual injury from having his Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) actual instances of identity fraud; (b) damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff James entrusted to Defendants as a condition for employment; (c) loss of his privacy; (d) imminent and impending injury arising from the ongoing and increased risk of fraud and identity theft; and (e) the time and expense of his mitigation efforts as a result of the Data Breach.

44. As a result of the Data Breach, Plaintiff James anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff James will continue to be at increased risk of identity theft and fraud for years to come.

45. Plaintiff James would not have entrusted his Sensitive Information to Defendants had he known they would fail to maintain adequate data security.

Plaintiff Sheehan

46. Plaintiff Sheehan was required to provide her Sensitive Information to Defendants in connection with her employment.

47. On or about July 2, 2021, Plaintiff Sheehan received notice from Defendants that her Sensitive Information—including her name, Social Security number, and driver's license or government-issued identification number—had been improperly exposed to unauthorized third parties. The notice received by Plaintiff Sheehan is substantially similar to the exemplar Notice of Data Breach letter submitted to the State of California.

48. As a direct result of the Data Breach, Plaintiff Sheehan has engaged in mitigation efforts and expended time and resources. Plaintiff Sheehan now checks her credit reports as well as her banking statements and credit card statements on a more frequent basis. This is valuable time Plaintiff Sheehan otherwise would have spent performing other activities, such as her job and/or leisure activities.

49. Knowing that thieves stole her Sensitive Information as part of the Data Breach and knowing that her Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiff Sheehan great anxiety. She is now very concerned about the theft of her identity. This Data Breach has given Plaintiff Sheehan hesitation about using electronic services and reservations about conducting other online activities requiring her personal information.

50. Plaintiff Sheehan suffered actual injury from having her Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of her Sensitive Information—a form of intangible property that Plaintiff Sheehan entrusted to Defendants as a condition for employment; (b) loss of her privacy;

(c) imminent and impending injury arising from the ongoing and increased risk of fraud and identity theft; and (d) the time and expense of her mitigation efforts as a result of the Data Breach.

51. As a result of the Data Breach, Plaintiff Sheehan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Sheehan will continue to be at increased risk of identity theft and fraud for years to come.

52. Plaintiff Sheehan would not have entrusted her Sensitive Information to Defendants had she known they would fail to maintain adequate data security.

Plaintiff Gamboa

53. Plaintiff Gamboa was required to provide her Sensitive Information to Defendants in connection with her employment.

54. On or about July 2, 2021, Plaintiff Gamboa received notice from Defendants that her Sensitive Information—including her name, Social Security number, and driver's license or government-issued identification number—had been improperly exposed to unauthorized third parties. The notice received by Plaintiff Gamboa is substantially similar to the exemplar Notice of Data Breach letter submitted to the State of California.

55. As a direct result of the Data Breach, Plaintiff Gamboa has engaged in mitigation efforts and expended time and resources. Plaintiff Gamboa now checks her credit reports as well as her banking statements and credit card statements on a more frequent basis. This is valuable time Plaintiff Gamboa otherwise would have spent performing other activities, such as her job and/or leisure activities.

56. Knowing that thieves stole her Sensitive Information as part of the Data Breach and knowing that her Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiff Gamboa great anxiety. She is now very concerned about the theft of her identity. This Data Breach has given Plaintiff Gamboa hesitation about using electronic services and reservations about conducting other online activities requiring her personal information.

57. Plaintiff Gamboa suffered actual injury from having her Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of her Sensitive Information—a form of intangible property that Plaintiff Gamboa entrusted to Defendants as a condition for employment; (b) loss of her privacy; (c) imminent and impending injury arising from the ongoing and increased risk of fraud and identity theft; and (d) the time and expense of her mitigation efforts as a result of the Data Breach.

58. As a result of the Data Breach, Plaintiff Gamboa anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Gamboa will continue to be at increased risk of identity theft and fraud for years to come.

59. Plaintiff Gamboa would not have entrusted her Sensitive Information to Defendants had she known they would fail to maintain adequate data security.

Plaintiff Williams

60. Plaintiff Williams was required to provide his Sensitive Information to Defendants in connection with his employment.

61. In or about July 2021, Plaintiff Williams received notice from Defendants that his Sensitive Information—including his name, Social Security number, and/or driver's license or government-issued identification number—had been improperly exposed to unauthorized third parties. The notice received by Plaintiff Williams is substantially similar to the exemplar Data Breach notice letters submitted to the various states Attorney Generals' offices, including the California and New Hampshire departments of justice.

62. As a direct result of the Data Breach, Plaintiff Williams has engaged in mitigation efforts and expended time and resources, including, but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and attempting to sign up for credit monitoring and identity theft protection services offered by Davaco; researching what he could do to stop future attacks; and contacting creditors and credit bureaus regarding numerous fraudulent attempts by unauthorized third parties to use his name and Social Security number to change his bank account passwords and gain access to his account. Plaintiff Williams now checks his credit reports as well as his banking statements and credit card statements on a more frequent basis. This is valuable time Plaintiff Williams otherwise would have spent performing other activities, such as his job and/or leisure activities.

63. As a result of the Data Breach, multiple unauthorized third parties attempted to use Plaintiff Williams' name and Social Security number to gain access to his bank account, make unauthorized withdrawals and purchases with his debit card linked to his bank account, and attempted check fraud on the account. Each attempt, beginning on or about August of 2021 and continuing through today, resulted in the loss of funds by Williams and hardship during the

time those funds were missing from the account. Moreover, as a result, Plaintiff Williams' credit score was materially and negatively impacted and has yet to recover to its pre-August 2021 level.

64. Plaintiff Williams has been forced to immediately take action and seek reimbursement from his bank for the loss of funds. He has spent his valuable time filing a police report in Colleen, Texas where some of the fraudulent transactions originated. Plaintiff Williams spent valuable time that he could have spent gainfully working following up on the same. Plaintiff Williams was forced to close his first account and open another account with a different account number, and prove to the bank that the charges were fraudulent. During the time between the fraud on the account and the bank's reimbursement, Mr. Williams was forced to find other methods of covering his expenses, such as borrowing money and forgoing necessities. Plaintiff Williams has spent at least forty-eight (48) total hours dealing with the Data Breach, valuable time Plaintiff Williams otherwise would have spent on other activities, including but not limited to work and/or recreation.

65. Knowing that thieves stole his Sensitive Information as part of the Data Breach and knowing that his Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiff Williams great anxiety. He is now very concerned about the theft of his identity. This Data Breach has given Plaintiff Williams hesitation about using electronic services and reservations about conducting other online activities requiring his personal information.

66. Plaintiff Williams suffered actual injury from having his Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) actual instances of identity fraud; (b) damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff Williams entrusted to Defendants as a condition for

employment; (c) loss of his privacy; (d) imminent and impending injury arising from the ongoing and increased risk of fraud and identity theft; (e) the time and expense of his mitigation efforts as a result of the Data Breach; and loss of monies taken from his account by fraudulent third party actors as a result of Defendants' negligence for a period of time (including loss of his ability to use the missing funds during that time).

67. As a result of the Data Breach, Plaintiff Williams anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Williams will continue to be at increased risk of identity theft and fraud for years to come.

68. Plaintiff Williams would not have entrusted his Sensitive Information to Defendants had he known they would fail to maintain adequate data security.

F. Defendants' Information Security Statement and Privacy Policies.

69. Defendants' policies detail their promises and legal obligations to maintain and protect employees' Sensitive Information.

70. Davaco's online privacy statement states in part that "DAVACO uses industry-standard efforts to safeguard the confidentiality of your personal information such as firewalls and authentication protection."[10]

71. Defendants also describe how they may use and disclose information—none of which provide them a right to expose Plaintiffs' and Class members' Sensitive Information to unauthorized third parties, such as was done in the Data Breach.

[10] Davaco's Site Usage and Privacy Statement, available at: https://www.davaco.com/legal (last accessed Jan. 7, 2022).

G. Defendants Knew or Should Have Known of the Risk Because Large Employers Are Particularly Susceptible to Cyber Attacks.

72. The number of U.S. data breaches surpassed 1,000 in 2016—a record high and a 40 percent increase in the number of data breaches from the previous year.[11] In 2019, 1,473 breaches were reported—an increase of 17 percent from the previous year.[12] That trend continues.

73. Defendants knew and understood unprotected or exposed Sensitive Information in the custody of employers, such as Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize Sensitive Information through unauthorized access. Indeed, when compromised, highly confidential related data is among the most sensitive and personally consequential.

74. As large employers, Defendants knew, or should have known, the importance of safeguarding Sensitive Information entrusted to them by Plaintiffs and Class members, and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

---

[11] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last accessed Jan. 7, 2022).

[12] Identity Theft Resource Center, *Identity Theft Resource Center®'s Annual End-of-Year Data Breach Report Reveals 17 Percent Increase in Breaches over 2018, available at:* https://www.idtheftcenter.org/post/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/ (last accessed Jan. 10, 2022).

H. Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' Sensitive Information.

75. Defendants acquire, collect, and store a massive amount of their employees' Sensitive Information—including Plaintiffs and Class members—such as protected confidential information and other personally identifiable data.

76. As a condition of employment, Defendants require their employees—including Plaintiffs and Class members—to entrust them with highly confidential Sensitive Information.

77. By requiring, obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Sensitive Information, Defendants assumed legal and equitable duties, and knew or should have known they were responsible for protecting Plaintiffs' and Class members' Sensitive Information from unauthorized access, disclosure, and/or acquisition.

78. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiffs and Class members relied on Defendants to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, to only allow authorized access and disclosure of this information, and prevent unauthorized access, disclosure, and/or acquisition of the information.

I. The Value of Sensitive Information and the Effects of Unauthorized Disclosure.

79. Defendants were well aware the Sensitive Information they collect is highly sensitive and of significant value to those who would use it for wrongful purposes.

80. Sensitive Information is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial fraud.[13] Indeed, a robust "cyber black market" exists

[13] *See* Federal Trade Commission, *What to Know About Identity Theft*, *available at*:

in which criminals openly post stolen Sensitive Information on multiple underground Internet websites, commonly referred to as the dark web.

81. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now–defunct AlphaBay,

> are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target.[14]

82. Consumers' Sensitive Information remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Sensitive Information has also been valued on the dark web at approximately $1 per line of information.[17]

---

https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Jan. 7, 2022).

[14] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed Jan. 7, 2022).

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 7, 2022).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 7, 2022).

[17] https://www.pacetechnical.com/much-identity-worth-black-market/#:~:text=Personally%20identifiable%20information%20is%20sold,at%20a%20fast%20

Alternatively, criminals are able to purchase access to entire company data breaches for $900 to $4,500.[18]

83. Individuals also rightfully place a high value not only on their Sensitive Information, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy—and the amount is considerable. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – $44.62."[19] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of Sensitive Information to bad actors—would be exponentially higher today.

84. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

85. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to

---

food%20joint (last accessed Jan. 7, 2022).

[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 7, 2022).

[19] Hann, Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last accessed Jan. 7, 2022).

apply for more credit in your name. Then, they use the credit cards and do not pay the bills, which damages your credit. You may not find out that someone is using your number until you are turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

86. The ramifications of Defendants' failure to keep Plaintiffs' and Class members' Sensitive Information secure are long lasting and severe. Because many of the data points stolen are persistent—for example, Social Security numbers and names—criminals who stole or purchase the Sensitive Information belonging to Plaintiffs and Class members do not need to immediately use the information to commit fraud. The Sensitive Information can be used or sold for use years later, and as such Plaintiffs and Class members will remain at risk for identity theft indefinitely.

87. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

88. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 7, 2022).

quickly inherited into the new Social Security number."[21] The Social Security Administration concurs, warning:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same . . . .
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[22]

89. Because of this, the information compromised in the Data Breach here is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

90. The Sensitive Information compromised in this Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[23]

---

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 7, 2022).

[22] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at*: http://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 7, 2022).

[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*:

91. Once Sensitive Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Sensitive Information being harvested from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim.

92. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet–enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[24] Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[25]

93. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

94. Data breaches facilitate identity theft as hackers obtain consumers' Sensitive Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' Sensitive Information to others who do the same.

95. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Sensitive Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[26] The GAO Report further notes that this type of identity fraud is the most

---

https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 7, 2022).

[24] FBI, *2019 Internet Crime Report Released, Data Reflects an Evolving Threat and the Importance of Reporting* (Feb. 11, 2020), *available at*: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Jan. 7, 2022).

[25] *Id.*

[26] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent,*

harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[27]

96. Additionally, the frequency of cyberattacks has increased significantly in recent years.[28] In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[29]

97. Cybersecurity Ventures, a leading researcher on cybersecurity issues,

> expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.[30]

98. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[31]

---

but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Jan. 7, 2022).

[27] *Id.*

[28] *See* https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (last accessed Jan. 7, 2022).

[29] https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last accessed Jan. 7, 2022) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).

[30] Cybercrime Magazine, *Cybercrime To Cost The World $10.5 Trillion Annually By 2020*, Nov. 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last accessed Jan. 7, 2022).

[31] Deloitte, *Impact of COVID-19 on Cybersecurity*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last accessed Jan. 7, 2022); Interpol, *Cyberthreats are constantly evolving in order to take*

99. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on Plaintiffs and the Class as a result of a breach.

J. Defendants Failed to Comply with FTC Guidelines.

100. The FTC promulgates numerous guides for businesses highlighting the importance of implementing reasonable data security practices for sensitive information ranging from personal information collected for employment to customer information.[32] According to the FTC, the need for data security should be factored into all business decision-making.[33]

101. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[34] The guidelines note businesses should protect the employee and customer sensitive personal information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

102. The FTC further recommends companies not maintain Sensitive Information longer than is needed for authorization of a transaction; limit access to sensitive data; require

---

advantage of online behaviour and trends. The COVID-19 outbreak is no exception, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last accessed Jan. 7, 2022).

[32] *See* Federal Trade Commission, *Start With Security: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Jan. 7, 2022).

[33] *Id.*

[34] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last accessed Jan. 7, 2022).

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[35]

103. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect employee and customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.[36] Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

104. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

105. Defendants were at all times fully aware of their obligation to protect employees and/or Plaintiffs' and Class members' Sensitive Information because of their position as national and international businesses and employers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

[35] FTC, *Start With Security*, *supra* note 31.

[36] *See* In Re CVS Caremark Corp., FTC File No. 072-3119; Complaint, available at: https://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf; *see also* Decision and Order, ¶ 4 ("a "consumer" shall include an "employee," and an individual seeking to become an employee . . . .") available at: https://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvsdo.pdf (last accessed Jan. 7, 2022)

K. Defendants Failed to Comply with Industry Standards.

106. Defendants failed to implement several basic cybersecurity safeguards that can be implemented to improve cyber resilience and require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) encrypting Sensitive Information; (b) educating and training employees on how to protect Sensitive Information; and (c) correctly configurating software and network devices.

107. Despite the abundance and availability of information regarding the threats and cybersecurity best practices to defend against those threats, Defendants chose to ignore them. These best practices were known, or should have been known by Defendants, whose failure to heed and properly implement industry standards directly led to the Data Breach and the unlawful exposure of Sensitive Information.

L. Plaintiffs' and Class Members' Sensitive Information Was Also Subject to a Ransomware Attack—a Distinct Form of Data Breach.

108. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the owner pays a fee to the perpetrator. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransom ware and it is critical to take precautions for protection."[37]

109. Ransomware attacks constitute data breaches in the traditional sense. For example, in a ransomware attack on the Florida city of Pensacola, and while the City was still recovering from the ransomware attack, hackers released 2GB of data files from the total 32GB of data that they claimed was stolen prior to encrypting the City's network with the maze

[37] *See How to Protect Your Networks from RANSOMWARE*, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Jan. 7, 2022).

ransomware. In the statement given to a news outlet, the hackers said, "***This is the fault of mass media who writes that we don't exfiltrate data*** . . . ."[38]

110. Other security experts agree that when a ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[39]

111. To prevent and detect ransomware attacks, including the ransomware attack that was part of this Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned

[38] *Pensacola Ransomware: Hackers Release 2GB Data as a Proof*, Cisomag (Dec. 27, 2019), *available at*: https://cisomag.eccouncil.org/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/ (emphasis added) (last accessed Jan. 7, 2022).

[39] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at*: https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed Jan. 7, 2022).

administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls-including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs m a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[40]

112. To prevent and detect ransomware attacks, including the ransomware attack that was part of this Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

[40] *Id.* at 3-4.

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[41]

[41] *See Security Tip (ST19-001) Protecting Against Ransomware* (original release date Apr. 11, 2019), emphasis in original, citations omitted, available at: https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Jan. 7, 2022).

113. To prevent and detect ransomware attacks, including the ransomware attack that was part of this Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> Secure internet-facing assets
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> Thoroughly investigate and remediate alerts
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> Include IT Pros in security discussions
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> Build credential hygiene
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> Apply principle of least-privilege
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events;
>
> Harden infrastructure
> - Use Windows Defender Firewall
> - Enable tamper protection
> - Enable cloud-delivered protection
> - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[42]

[42] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Jan. 7, 2022).

114. Given Defendants were storing the Sensitive Information of over ten thousand current and former employees, Defendants knew or should have known to implement all of the above measures to prevent and detect ransomware attacks.

115. The ransomware attack on Defendants included Plaintiffs' and Class members' Sensitive Information stored on Defendants' computer system. As part of the Defendants' notice to Plaintiffs and Class members about the Data Breach, Defendants admitted the breach included a ransomware attack and the unknown actor "viewed and removed" Plaintiffs' and Class members' Sensitive Information. Therefore, an unauthorized party now possesses Plaintiffs' and Class members' Sensitive Information because, as previously stated, even if Defendants or the unauthorized party claim the exfiltrated data was deleted, "Proof of deletion is not a thing."[43]

M. Plaintiffs and Class Members Suffered Damages.

116. The ramifications of Defendants' failure to keep Plaintiffs' and Class members' Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[44]

117. The Sensitive Information belonging to Plaintiffs and Class members is private, sensitive in nature, and was left inadequately protected by Defendants, who did not obtain Plaintiffs' or Class members' consent to disclose their Sensitive Information to any other person as required by applicable law and industry standards.

---

[43] *See* Keith Mukai, *ArbiterSports Was Hacked. Don't Use Them Ever Again*, Medium (Aug. 29, 2020), *available at*: https://medium.com/@kdmukai_64726/arbitersports-was-hacked-dont-use-them-ever-again-fddea92bcd21 (last accessed Jan. 7, 2022).

[44] 2014 LexisNexis® True Cost of Fraud℠ Study, *Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs*, *available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Jan. 7, 2022).

118. The Data Breach was a foreseeable direct and proximate result of Defendants' failure to:

a. properly safeguard and protect Plaintiffs' and Class members' Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law;

b. establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Sensitive Information; and

c. protect against reasonably foreseeable threats to the security or integrity of such information.

119. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligation to protect Plaintiffs' and Class members' Sensitive Information.

120. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of the Sensitive Information.

121. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiffs and Class members have been placed at ongoing, imminent, and immediate increased risk of harm from identity theft and fraud, requiring them to take time they otherwise would have dedicated to other life demands, such as work, leisure, and family, in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

122. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more

resolving problems," and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[45]

123. As a result of Defendants' failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. the compromise, publication, theft, and/or unauthorized use of their Sensitive Information;

b. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. lost opportunity costs and lost wages associated with efforts expended, and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. the current and ongoing risk to their Sensitive Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Sensitive Information;

e. current and future costs in terms of time, effort, and money that will be expended to prevent, mitigate, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class members' lives; and

[45] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Jan. 7, 2022).

f. stress, anxiety, and other related forms of emotional distress.

124. In addition to a remedy for these harms, Plaintiffs and the Class members maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and/or theft.

CLASS ACTION ALLEGATIONS

125. Plaintiffs seek relief on behalf of themselves and as representatives of all others similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a Nationwide class, defined as follows:

> All individuals residing in the United States whose Sensitive Information was compromised in the data breach first announced by Defendants on or about July 2, 2021 (the "Nationwide Class").

126. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of the following state of California subclass ("California Subclass"):

> All individuals residing in the state of California whose Sensitive Information was compromised in the data breach first announced by Defendants on or about July 2, 2021.

127. Where appropriate, the Nationwide Class and state subclass are collectively referred to as the "Class."

128. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the Judge(s) and Court personnel in this case and any members of their immediate families.

129. Plaintiffs reserve the right to amend the class definitions, including creating additional subclasses as necessary, after having had an opportunity to conduct discovery.

130. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

131. All Class members are readily ascertainable in that Defendants have access to addresses and other contact information for all Class members, which can be used for providing notice to Class members.

132. **Numerosity.** Consistent with Fed. R. Civ. P. 23(a)(1), the class members are so numerous and geographically dispersed that joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class includes approximately 14,578 individuals whose Sensitive Information was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court–approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

133. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and 23(b)(3), this action involves common questions of law and fact predominating over any questions that may affect only individual Class members. Common questions include:

a. whether Defendants engaged in the wrongful conduct alleged herein;

b. whether Defendants' inadequate data security measures were a cause of the Data Breach;

c. whether Defendants' conduct was negligent;

d. whether Defendants' conduct was unlawful;

e. whether Defendants owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their Sensitive Information;

f. whether Defendants owed a contractual duty to Plaintiffs and Class members to protect their Sensitive Information;

g. whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their Sensitive Information;

h. whether Defendants breached contractual duties owed to Plaintiffs and Class members to protect their Sensitive Information;

i. whether Defendants had a duty to provide prompt and accurate notice of the Data Breach to Plaintiffs and Class members;

j. whether Defendants breached their duty to provide prompt and accurate notice of the Data Breach to Plaintiffs and Class members;

k. whether Plaintiffs and Class members are at a present and/or future increased risk for identity theft because of the Data Breach;

l. whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class members' Sensitive Information in violation Section 5 of the FTC Act;

m. whether Plaintiffs and Class members suffered injury, including ascertainable losses, as a result of Defendants' conduct (or failure to act);

n. whether Plaintiffs and Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

o. whether Plaintiffs and Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

134. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of the claims of other Class members in that Plaintiffs, like all Class members, had their Sensitive Information compromised, viewed, breached, and stolen in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members, and Plaintiffs assert the same claims and forms of relief as the Class.

135. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs are members of the Class defined herein; are committed to vigorously pursuing this matter against Defendants to obtain relief for the Class; and have no interests that are antagonistic to, or in conflict with, the interests of other Class members. Plaintiffs retained counsel who are competent and experienced in litigating class actions and complex litigation, including privacy litigation of this kind. Plaintiffs and their counsel intend to vigorously prosecute this case, and will fairly and adequately protect the Class's interests.

136. **Superiority.** Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their individual claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in

the aggregate would go unremedied without certification of the Class. Plaintiffs and Class members were harmed by Defendants' wrongful conduct, action, and/or inaction. Litigating this action as a class action will reduce the possibility of inconsistent outcomes of individual actions, and repetitious litigation relating to Defendants' conduct, action, and/or inaction. Plaintiffs are unaware of any difficulties that might be encountered in this litigation that would preclude its maintenance as a class action.

137. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the common questions of law and fact predominate over any questions affecting individual Class members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

138. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants, through their uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendants continue to maintain their inadequate security practices, retain possession of Plaintiffs' and Class members' Sensitive Information, and have not been forced to change their practices or relinquish Sensitive Information by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

139. Likewise, particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Plaintiffs' and Class members' Sensitive Information was accessed and/or acquired by an unauthorized party in the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and Class members;

c. Whether Defendants failed to take adequate and reasonable steps to safeguard Plaintiffs' and Class members' Sensitive Information;

d. Whether Defendants failed to adequately monitor their data security systems;

e. Whether Defendants failed to comply with applicable laws, regulations, and/or industry standards relating to data security amounting to negligence;

f. Whether Defendants' security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

g. Whether Defendants knew or should have known that they did not employ adequate and reasonable measures to keep Plaintiffs' and Class members' Sensitive Information secure; and

h. Whether Defendants' failure to adhere to FTC data security obligations, industry standards, and/or measures recommended by data security experts caused the Data Breach.

CAUSES OF ACTION

Count I

Negligence
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

140. Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

141. Defendants collected, maintained, and used Plaintiffs' and Class members' Sensitive Information, and by doing so undertook and owed a duty to Plaintiffs and Class

members to exercise reasonable care to secure and safeguard their Sensitive Information, and to use industry standard, commercially available, and reasonable methods to do so. At all times, Defendants knew Plaintiffs' and Class members' Sensitive Information was private and confidential, was required to be kept private and confidential, and the types of harm Plaintiffs and Class members could and would suffer if the Sensitive Information was wrongfully disclosed.

142. Defendants owed a duty of care not to subject Plaintiffs and Class members, along with their Sensitive Information, to an unreasonable risk of harm because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices by Defendants.

143. Because of their duty of care to prevent foreseeable harm to Plaintiffs and Class members, and Defendants therefore had, and still has, a duty to take adequate and reasonable steps to safeguard their Sensitive Information from unauthorized access and/or acquisition (theft). More specifically, this duty includes:

a. Exercising reasonable care in the hiring, training, and/or supervising of their employees and agents entrusted with access to and safeguarding of Plaintiffs' and Class members' Sensitive Information on cyber security measures and industry standards regarding the safety and safeguarding of Sensitive Information;

b. Designing, maintaining, and testing Defendants' data security systems, data storage architecture, and data security protocols to ensure Plaintiffs' and Class members' Sensitive Information in Defendants' possession

was and is adequately secured and protected from unauthorized access and/or acquisition;

c. Implementing processes to timely and adequately detect an unauthorized breach of Defendants' security systems and data storage architecture;

d. Timely acting on all suspicions, warnings, and alerts, including public information, regarding Defendants' security vulnerabilities and potential compromise of Plaintiffs' and Class members' Sensitive Information in their possession; and

e. Maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

144. Defendants had a common law duty to prevent foreseeable harm to Plaintiffs and Class members. The duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices of Defendants in their affirmative collecting, maintaining, and using of Plaintiffs' and Class members' Sensitive Information. In fact, not only was it foreseeable that Plaintiffs and Class members would be harmed by Defendants' failure to protect their Sensitive Information because unauthorized parties, hackers, and other malicious actors routinely attempt to access and steal such information for use in nefarious purposes, but Defendants also knew it was more likely than not that Plaintiffs and Class members would be harmed as a result.

145. Defendants knew, or should have known, of the risks inherent in collecting, maintaining, and using Sensitive Information, the vulnerabilities of their data security systems, and the importance of adequate and industry standard security. Defendants knew or should have known about numerous, well-publicized data breaches and of industry security warnings.

146. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' Sensitive Information.

147. Defendants' duties to use adequate and reasonable security measures also arose as a result of the special relationship existing between them, on the one hand, and Plaintiffs and Class members, on the other hand. This special relationship, recognized in laws and regulations, arose by virtue of Plaintiffs and Class members being current or former employees of Defendants. Plaintiffs and Class members reasonably believed that Defendants—as their employers—would take adequate security precautions to protect their Sensitive Information. Defendants alone had the duty to and could have ensured their security system and data storage architecture was sufficient to prevent or minimize the Data Breach.

148. Further, the policy of preventing future harm weighs in favor of finding a special relationship between Defendants on the one hand, and Plaintiffs and Class members on the other. If companies are not held accountable for failing to implement minimum industry-standard security practices and procedures to safeguard Sensitive Information in their possession, companies will have no incentive to—and ultimately will not—take the necessary steps to protect against future security breaches.

149. Defendants also owed a duty to timely disclose the material fact that their computer network and data security practices and protocols were inadequate to safeguard Plaintiffs' and Class members' Sensitive Information from unauthorized access and acquisition.

150. Defendants also had independent duties under state and federal laws requiring them to reasonably safeguard Plaintiffs' and Class members' Sensitive Information, and promptly notify them about the data breach.

151. Defendants solicited, gathered, stored, and used Plaintiffs' and Class members' Sensitive Information to in their normal course of business—which affects commerce.

152. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, and/or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Sensitive Information. Defendants also breached their duty to Plaintiffs and Class members to adequately protect and safeguard Sensitive Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to and acquisition of unsecured Sensitive Information. Defendants breached these duties through the conduct alleged in this Complaint by, including without limitation:

a. failing to protect the Sensitive Information in their possession;
b. failing to implement the minimum industry-standard security practices and procedures;
c. failing to maintain adequate computer systems and data security practices to safeguard the Sensitive Information in their possession despite knowing their vulnerabilities;
d. allowing unauthorized access to and acquisition of Plaintiffs' and Class members' Sensitive Information;
e. failing to implement adequate system and event monitoring;
f. failing to disclose the material fact that their computer systems and data security practices were inadequate to safeguard the Sensitive Information in their possession from unauthorized access and acquisition; and

g. failing to disclose the material fact of the Data Breach to Plaintiffs and Class members in an accurate manner.

153. Furthering Defendants' negligent practices, Defendants also breached their duties by failing to implement adequate security supervision and oversight of the Sensitive Information with which they were and are entrusted—in spite of the known risk and foreseeable likelihood of breach and misuse—that permitted an unauthorized party to access and acquire Plaintiffs' and Class members' Sensitive Information, and intentionally disclose the Sensitive Information to an unauthorized party without prior consent.

154. The injuries suffered by Plaintiffs and Class members were proximately and directly caused by Defendants' breach of their duties—specifically their failure to exercise adequate and reasonable care in hiring, training, and/or supervising their employees and agents tasked with safeguarding and/or with access to Plaintiffs' and Class members' Sensitive Information, failure to monitor and/or test their data security system, and failure to monitor or otherwise follow reasonable industry standard security measures to protect Plaintiffs' and Class members' Sensitive Information.

155. When individuals—such as Plaintiffs and Class members—have their personal information stolen, they are placed at current and ongoing risk of identity theft, and need to take steps to protect themselves, including, for example, paying for credit monitoring services, and purchasing or obtaining credit reports to protect themselves from identity theft. The credit monitoring services and purchasing or obtaining credit reports are required because of the present economic risk and harm—unauthorized parties exfiltrated Sensitive Information enabling them to commit identity theft, and secure fraudulent loans, leases, and credit cards. And, the unauthorized parties are currently and likely to continue attempting their identity theft and

fraudulent activities for the foreseeable future, so Plaintiffs and Class members have been injured and are exposed to a real risk of misuse of their Sensitive Information.

156. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class members, their Sensitive Information would not have been accessed and acquired by an unauthorized party. And as a direct and proximate result of Defendants' failure to exercise adequate and reasonable care and use industry standard, commercially available, adequate, and reasonable security measures, Plaintiffs' and Class members' Sensitive Information was accessed and acquired by an unauthorized party who has and likely will continue to use the information to commit identity or financial fraud. Plaintiffs and Class members face the ongoing concrete, imminent, and impending substantially heightened risk of identity theft, fraud, and misuse of their Sensitive Information.

157. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect Plaintiffs' and Class members' Sensitive Information, and the harm suffered and/or risk of imminent harm suffered by Plaintiffs and Class members.

158. It was foreseeable Defendants' failure to exercise reasonable care to safeguard the Sensitive Information in their possession and/or control would lead to one or more types of injury to Plaintiffs and Class members. And the Data Breach was foreseeable given the known, publicized, high frequency of cyberattacks and data breaches against companies accessing, maintaining, storing, and/or utilizing Sensitive Information.

159. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of, or should have known of, the inherent risks in collecting, storing, and using Sensitive Information, the critical importance of providing adequate security for Sensitive Information, the current cyber scams being perpetrated

using Sensitive Information, and their own inadequate security practices, procedures, and protocols in place to secure Plaintiffs' and Class members' Sensitive Information.

160. Plaintiffs and Class members have no ability to protect their Sensitive Information in Defendants' possession.

161. Defendants alone were in a position to protect against the harm and injuries suffered by Plaintiffs and Class members as a result of the Data Breach.

162. As a direct and proximate result of Defendants' conduct and violations of the above–mentioned statutes, Plaintiffs and Class members have suffered, and continue to suffer, damages arising from the Data Breach as described herein, and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial. Such injuries and damages include but are not limited to those described above, including:

a. actual identity theft, and current and ongoing risk of identity fraud;

b. loss of the opportunity to control how their Sensitive Information is used;

c. the compromise, publication, and/or theft of their Sensitive Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. lost opportunity costs associated with the efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely

reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. the current and ongoing risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Sensitive Information in Defendants' continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and stolen by an unauthorized party as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. the diminished value of their Sensitive Information;

j. other economic harm;

k. emotional distress; and

l. the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

163. The nature of other forms of damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft of the Sensitive Information during the Data Breach mentioned above.

Count II

Invasion of Privacy
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

164. Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

165. Plaintiffs and Class members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

166. Defendants owed a duty to Plaintiffs and Class members to keep their Sensitive Information confidential.

167. The unauthorized release of Sensitive Information is highly offensive to a reasonable person.

168. The intrusion was into a place or thing that was private and is entitled to be private. Plaintiffs and Class members disclosed their Sensitive Information to Defendants as part of their employment—but privately—with the intention that the Sensitive Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

169. The Data Breach constitutes an intentional interference with Plaintiffs' and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

170. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

171. Acting with knowledge, Defendants had notice and knew their inadequate cybersecurity practices would cause injury to Plaintiffs and Class members.

172. As a proximate result of Defendants' acts and omissions, Plaintiffs and Class members' Sensitive Information was disclosed to, and used by, third parties without authorization, causing Plaintiffs and Class members to suffer damages.

173. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that the Sensitive Information maintained by Defendants may be breached again—leading to further viewing, distributing, and use of updated and additional Sensitive Information by unauthorized persons.

174. Plaintiffs and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class members.

Count III

Breach of Implied Contract
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

175. Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

176. Defendants required Plaintiffs and Class members to provide their personal and Sensitive Information, including names, addresses, Social Security numbers, driver's license numbers and/or government issued identification numbers, and other Sensitive Information, as a condition of their employment.

177. As a condition of their employment with Defendants, Plaintiffs and Class members provided their Sensitive Information. In so doing, Plaintiffs and Class members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately

notify Plaintiffs and Class members if their data had been accessed, viewed, compromised, stolen, and/or disseminated to an unauthorized party.

178. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants. Defendants did not.

179. Defendants breached the implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect their Sensitive Information, and by failing to provide timely and accurate notice to them that their Sensitive Information was accessed, viewed, and stolen as a result of the Data Breach.

180. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class members have suffered, and continue to suffer, damages arising from the Data Breach as described herein, and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial. Such injuries and damages include but are not limited to those described above, including:

a. actual identity theft, and current and ongoing risk of identity fraud;

b. loss of the opportunity to control how their Sensitive Information is used;

c. the compromise, publication, and/or theft of their Sensitive Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. lost opportunity costs associated with the efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft,

placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. the current and ongoing risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Sensitive Information in Defendants' continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and stolen by an unauthorized party as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. the diminished value of their Sensitive Information;

j. other economic harm;

k. emotional distress; and

l. the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

Count IV

Unjust Enrichment
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

181. Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

182. Defendants benefited from receiving Plaintiffs' and Class member's Sensitive Information by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

183. Defendants also understood and appreciated that Plaintiffs' and Class members' Sensitive Information was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that Sensitive Information.

184. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of their employment, and in connection thereto, by providing their Sensitive Information to Defendants with the understanding that Defendants would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendants with their Sensitive Information. In exchange, Plaintiffs and Class members should have received adequate protection and data security for such Sensitive Information held by Defendants.

185. Defendants knew Plaintiffs and Class members conferred a benefit that Defendants accepted. Defendants profited from these transactions and used Plaintiffs' and Class members' Sensitive Information for business purposes.

186. Defendants failed to provide reasonable security, safeguards, and protections to Plaintiffs' and Class members' Sensitive Information.

187. Under the principles of equity and good conscience, Defendants should not be permitted to retain money belonging to Plaintiffs and Class members, because Defendants

failed to implement appropriate data management and security measures mandated by industry standards.

188. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class members.

189. Defendants' enrichment at the expense of Plaintiffs and Class members is and was unjust.

190. Plaintiffs and Class members have no adequate remedy at law.

191. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to:

a. actual identity theft, and current and ongoing risk of identity fraud;

b. loss of the opportunity to control how their Sensitive Information is used;

c. the compromise, publication, and/or theft of their Sensitive Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. lost opportunity costs associated with the efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. the current and ongoing risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Sensitive Information in Defendants' continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and stolen by an unauthorized party as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. the diminished value of their Sensitive Information;

j. other economic harm;

k. emotional distress; and

l. the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

192. As a result of Defendants' wrongful conduct, as previously alleged, Plaintiffs and Class members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

Count V

Breach of Fiduciary duty
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

193. Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

194. In light of their special relationship, Defendants became the guardian of Plaintiffs' and Class members' Sensitive Information. Defendants became fiduciaries, created by their undertaking and guardianship of their employees' Sensitive Information, to act primarily for the benefit of those employees, including Plaintiffs and Class members. This duty included the obligation to safeguard Plaintiffs' and Class members' Sensitive Information and to timely detect and notify them in the event of a data breach.

195. In order to provide Plaintiffs and Class members compensation and employment benefits, or to consider Plaintiffs and Class members for employment, Defendants required Plaintiffs and Class members to provide their Sensitive Information to Defendants.

196. Defendants knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class members' Sensitive Information for the benefit of Plaintiffs and Class members in order to provide Plaintiffs and Class members compensation and employment benefits.

197. Defendants have fiduciary duties to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship with them. Defendants breached their fiduciary duties owed to Plaintiffs and Class members by failing to properly encrypt and otherwise protect Plaintiffs' and Class members' Sensitive Information. Defendants further breached their fiduciary duties owed to Plaintiffs and Class members by failing to timely detect the Data Breach and notify and/or warn Plaintiffs and Class members of the Data Breach.

198. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered or will suffer injury, including but not limited to:

a. actual identity theft, and current and ongoing risk of identity fraud;

b. loss of the opportunity to control how their Sensitive Information is used;

c. the compromise, publication, and/or theft of their Sensitive Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. lost opportunity costs associated with the efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. the current and ongoing risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Sensitive Information in Defendants' continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and stolen by an unauthorized party as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. the diminished value of their Sensitive Information;

j. other economic harm;

k. emotional distress; and

l. the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

199. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Count VI

Breach of Confidence
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

200. Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

201. At all times during Plaintiffs' and Class members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiffs' and Class members' Sensitive Information that Plaintiffs and Class members provided to Defendants.

202. As alleged herein and above, Defendants' relationship with Plaintiffs and Class members was governed by terms and expectations that Plaintiffs' and Class members' Sensitive Information would be collected, stored, maintained, and used, in confidence and protected—and would not be disclosed to unauthorized third parties.

203. Plaintiffs and Class members provided their respective Sensitive Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

204. Plaintiffs and Class members also provided their Sensitive Information to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect their Sensitive Information from unauthorized disclosure, such as following basic principles and industry standards to protect their networks and data systems.

205. Defendants required and voluntarily received, in confidence, Plaintiffs' and Class members' Sensitive Information with the understanding the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

206. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and Class members' Sensitive Information, Plaintiffs' and Class members' Sensitive Information was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

207. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and Class members have suffered, and will continue to suffer damages.

208. But for Defendants' disclosure of Plaintiffs' and Class members' Sensitive Information in violation of the parties' understanding of confidence, Plaintiffs' and Class members' Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' Sensitive Information, as well as the resulting damages.

209. The injury and harm Plaintiffs and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class members' Sensitive Information. Defendants knew or should have known their computer systems and technologies for accepting and securing Plaintiffs' and Class members' Sensitive Information was inadequate and had numerous security and other vulnerabilities placing Plaintiffs' and Class members' Sensitive Information in jeopardy.

210. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to:

a. actual identity theft, and current and ongoing risk of identity fraud;

b. loss of the opportunity to control how their Sensitive Information is used;

c. the compromise, publication, and/or theft of their Sensitive Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information;

e. lost opportunity costs associated with the efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. the current and ongoing risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Sensitive Information in Defendants' continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information accessed and stolen by an unauthorized party as a result of the Data Breach—which may take months if not years to discover, detect, and remedy;

h. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their Sensitive Information;

i. the diminished value of their Sensitive Information;

j. other economic harm;

k. emotional distress; and

l. the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

211. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Count VII

Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On behalf of California Plaintiffs and the California Subclass)

212. California Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

213. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent the unauthorized access, exfiltration, theft, and/or disclosure of California Plaintiffs' and California Subclass members' Sensitive Information as a result of Defendants' violation of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect California Plaintiffs' and California Subclass members' Sensitive Information.

214. As a direct and proximate result of Defendants' acts, California Plaintiffs' and California Subclass members' Sensitive Information was subjected to unauthorized access and exfiltration, theft, and/or disclosure as a result of Defendants' violation of the duty.

215. As a direct and proximate result of Defendants' acts and/or failures to act, California Plaintiffs and California Subclass members were injured and lost money or property, including but not limited to the loss of California Plaintiffs' and California Subclass members' legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described above.

216. Defendants knew or should have known that their network computer systems and data security practices were inadequate to safeguard California Plaintiffs' and California Subclass members' Sensitive Information, and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices

appropriate to the nature of the information to protect California Plaintiffs' and California Subclass members' Sensitive Information.

217. Defendants are organized for the profit or financial benefit of their owners and collect personal information as defined in Cal. Civ. Code § 1798.140.

218. California Plaintiffs' and California Subclass members' Sensitive Information includes "Personal Information" as defined in Cal. Civ. Code § 1798.140.

219. California Plaintiffs and California Subclass members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard California Plaintiffs' and California Subclass members' Sensitive Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold California Plaintiffs' and California Subclass members' Sensitive Information. California Plaintiffs and California Subclass members have an interest in ensuring their Sensitive Information is reasonably protected.

220. In addition, on November 30, 2021, California Plaintiffs Sheehan and Gamboa, by and through their counsel, each sent a notice letter to Davaco's registered service agent via FedEx next day air. On information and belief, Defendants did not cure the Data Breach within 30 days, and California Plaintiffs do not believe any such cure was or is possible under these facts and circumstances. California Plaintiffs seek actual damages and/or statutory damages of no less than $100 and up to $750 per employee record subject to the Data Breach, on behalf of the California Class, as authorized by the CCPA.

Count VIII

Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of California Plaintiffs and the California Subclass)

221. California Plaintiffs incorporate paragraphs 1 through 139 as though fully set forth herein.

222. Defendants violated California Business and Professions Code § 17200, *et seq*., by engaging in unlawful, unfair, or fraudulent business acts and practices, and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200 by reason of the conduct alleged herein.

223. Defendants stored California Plaintiffs' and California Subclass members' Sensitive Information in their network environment. Defendants falsely represented to California Plaintiffs and California Class members that their Sensitive Information was secure and would remain private or, alternatively, failed to disclose to California Plaintiffs and California Subclass members that their Sensitive Information was not secure.

224. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures in compliance with federal regulations and that would have kept California Plaintiffs' and California Subclass members' Sensitive Information secure and prevented the loss or misuse of that Sensitive Information.

225. Even without these misrepresentations and omissions, California Plaintiffs and California Subclass members were entitled to assume, and did assume, Defendants would take appropriate measures to keep their Sensitive Information safe. Defendants did not disclose at any time that California Plaintiffs' and California Subclass members' Sensitive Information was vulnerable to hackers because Defendants' data security measures were inadequate and most

likely outdated, and Defendants were the only ones in possession of that material information, which they had a duty to disclose.

A. Unlawful Business Practices

226. Defendants violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, both by affirmative conduct and by omission, the safety of their network environment, specifically the security thereof, and their ability to safely store California Plaintiffs' and California Subclass members' Sensitive Information.

227. Defendants also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and/or by failing to provide timely and accurate notice to California Plaintiffs and California Subclass members of the Data Breach.

228. Defendants also violated California Civil Code § 1798.81.5(b) in that they failed to maintain reasonable security procedures and practices.

229. If Defendants had complied with these legal requirements, California Plaintiffs and California Subclass members would not have suffered the damages related to the Data Breach, and from Defendants' failure to provide timely and accurate notice to California Plaintiffs and California Subclass members of the Data Breach.

230. Defendants' acts, omissions, and/or misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

231. California Plaintiffs and California Subclass members suffered injury in fact and lost money and/or property as the result of Defendants' unlawful business practices. In addition, California Plaintiffs' and California Subclass members' Sensitive Information was accessed, viewed, and taken—and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear the hacked information is of tangible value. California Plaintiffs and California Subclass members also suffered consequential out-of-pocket losses for procuring credit freezes and/or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

B. Unfair Business Practices

232. Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and/or omissions greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and misrepresentations to California Plaintiffs and California Subclass members about Defendants' data security cannot be said to have had any utility at all. The actions and/or omissions were clearly injurious to California Plaintiffs and California Subclass members, directly causing the harms.

233. Defendants also engaged in unfair business practices under the "tethering test." Defendants' actions and/or omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See*, *e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the

Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and/or omissions thus amount to a violation of the law.

234. Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and/or omissions, as described in detail above, is substantial in that it affects California Plaintiffs and California Subclass members and caused those persons to suffer harms. Such harms include, but are not limited to, an ongoing and substantial risk of identity theft, disclosure of California Plaintiffs' and California Subclass members' Sensitive Information to third parties without their consent, diminution in value of their Sensitive Information, consequential out-of-pocket losses for among other things, procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to the unauthorized disclosure of their Sensitive Information.

235. This harm continues given the fact that California Plaintiffs' and California Subclass members' Sensitive Information remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without California Plaintiffs' and California Subclass members' consent. Defendants' actions and/or omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also*, *e.g.*, *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

236. California Plaintiffs and California Subclass members suffered injury in fact and lost money and/or property as the result of Defendants' unfair business practices. California

Plaintiffs' and California Subclass members' Sensitive Information was accessed, viewed, and taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear the hacked information is of tangible value. California Plaintiffs and California Subclass members have also suffered harm as detailed herein.

237. As a result of Defendants' unlawful and unfair business practices in violation of the UCL, California Plaintiffs and California Class members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

Count IX

Declaratory and Injunctive Relief
(On Behalf of Plaintiffs, the Nationwide Class, and California Subclass)

238. Plaintiffs incorporate paragraphs 1 through 237 as though fully set forth herein.

239. Plaintiffs bring this cause of action under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

240. As previously alleged, Plaintiffs and Class members entered into an implied contract requiring Defendants to provide adequate security for the Sensitive Information it collected from Plaintiffs and Class members.

241. Defendants owe a duty of care to Plaintiffs and Class members, requiring Defendants to adequately secure Plaintiffs' and Class members' Sensitive Information.

242. Defendant still possess Plaintiffs' and Class members' Sensitive Information.

243. Since the Data Breach, Defendants have announced few if any changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices that permitted the Data Breach to occur and, thereby, prevent future data breaches.

244. Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Defendants' insufficient data security is known to hackers, the Sensitive Information in Defendants' possession is even more vulnerable to cyberattack.

245. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs' and Class members' Sensitive Information. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their Sensitive Information and Defendants' failure to address the security failings that led to such exposure.

246. There is no reason to believe Defendants' security measures are any more adequate to meet their contractual obligations and legal duties now than they were before the Data Breach.

247. Plaintiffs, therefore, seek a declaration (1) that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to ordering Defendants:

a. engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. engage third-party security auditors and internal personnel to run automated security monitoring;

c. audit, test, and train their security personnel regarding any new or modified procedures;

d. segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. purge, delete, and destroy in a reasonably secure manner employee data not necessary for their provisions of services;

f. conduct regular computer system scanning and security checks;

g. routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their Sensitive Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of themselves and all others similarly situated, respectfully requests that the Court enter an order:

i. Certifying the proposed Classes as requested herein;

j. Appointing Plaintiffs as Class Representatives and the undersigned counsel as Class Counsel;

k. Finding that Defendants engaged in the unlawful conduct as alleged herein;

l. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete, destroy, and purge Plaintiffs' and Class members' Sensitive Information unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

iv. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiffs' and Class members' Sensitive Information;

v. prohibiting Defendants from maintaining Plaintiffs' and Class members' Sensitive Information on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of their network is compromised, hackers cannot gain access to other portions of their systems;

x. requiring Defendants to conduct regular database scanning and security checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Sensitive Information, as well as protecting Plaintiffs' and Class members' Sensitive Information;

xii. requiring Defendants to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting Sensitive Information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats they face as a result of the loss of their confidential Sensitive Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to design, maintain, and test their computer systems to ensure Sensitive Information in their possession is adequately secured and protected;

xvii. requiring Defendants to detect and disclose any future data breaches in a timely and accurate manner;

xviii. requiring Defendants to implement multi-factor authentication requirements, if not already implemented;

xix. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; and

xx. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Plaintiffs and Class members.

m. Awarding Plaintiffs and Class members damages and the members of the California Class statutory damages;

n. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

o. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

p. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Date: January 10, 2022

Respectfully Submitted,

/s/ Rachele R. Byrd

Rachele R. Byrd (*Pro Hac Vice*)
byrd@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Tele: 619.239.4599
Fax: 619.234.4599

Gayle M. Blatt (*Pro Hac Vice*)
gmb@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel: 619.238.1811
Fax: 619.544.9232

M. Anderson Berry (*Pro Hac Vice*)
aberry@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Tel: 916.239.4778
Fax: 916.924.1829

Joshua B. Swigart (*Pro Hac Vice*)
josh@swigartlawgroup.com
SWIGART LAW GROUP, APC
2221 Camino Del Rio S., Suite 308
San Diego, CA 92108
Tel: 866.219.3343
Fax: 866.219.8344

Balon B. Bradley (Bar No. 02821700)
balon@bbradleylaw.com
BALON B. BRADLEY LAW FIRM
11910 Greenville Ave., Suite 220
Dallas, TX 75243
Tel: 972.991.1582
Fax: 972.755.0424

Attorneys for Plaintiffs and the Class